United States District Court
District of New Jersey

ORIGINAL FILED

AUG - 1 2012

PATTY SHWARTZ
U.S. MAG. JUDGE

UNITED STATES OF AMERICA	:	Hon. Patty Shwartz
v.	:	Magistrate No. 12-3043
DMITRIY SMILIANETS	:	**SECOND AMENDED CRIMINAL COMPLAINT**
a/k/a [redacted] a/k/a a/k/a a/k/a a/k/a a/k/a	:	FILED UNDER SEAL

I, Jeremiah Reppert, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief.

SEE ATTACHMENT A

I further state that I am a Special Agent with the United States Secret Service, and that this complaint is based on the following facts:

SEE ATTACHMENT B

JEREMIAH REPPERT
Special Agent
United States Secret Service

Sworn to before me and subscribed in my presence,

August 1, 2012 at Newark, New Jersey
Date City and State

Honorable Patty Shwartz
United States Magistrate Judge

ATTACHMENT A

COUNT I

Between in or about December 2003 and in or about August 2005, in Hudson County, in the District of New Jersey; and elsewhere, defendant

DMITRIY SMILIANETS,
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]

did knowingly and intentionally conspire and agree with others to:

(1) having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, any writings, signs, signals, pictures, and sounds for the purpose of executing such scheme or artifice in a manner affecting a financial institution, contrary to Title 18, United States Code, Section 1343; and

(2) execute a scheme and artifice to defraud financial institutions, and to obtain the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, financial institutions, by means of materially false and fraudulent pretenses, representations, and promises, contrary to Title 18, United States Code, Section 1344.

In violation of Title 18, United States Code, Section 1349.

COUNT II

Between in or about February 2008 and in or about November 2008, in the United States and elsewhere, defendant

DMITRIY SMILIANETS,
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]

did knowingly and intentionally conspire and agree with others to transfer, possess and use means of identification of other persons without lawful authority, in a manner affecting interstate and foreign commerce, with the intent to commit, and in connection with, unlawful activity constituting a violation of federal law, namely, Title 18, United States Code, Section 1343, contrary to Title 18, United States Code, Sections 1028(a)(7).

In violation of Title 18, United States Code, Sections 1028(f).

COUNT III

Between in or about October 2006 and in or about July 2012, in Mercer and Middlesex Counties, in the District of New Jersey, and elsewhere, defendant

DMITRIY SMILIANETS,
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]
a/k/a [redacted]

did knowingly and intentionally conspire and agree with each other, Albert Gonzalez, Patrick Toey, CC #1, CC#2, and others to devise a scheme and artifice to defraud corporate victims, their customers, and the financial institutions that issued credit and debit cards to those customers, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing the scheme and artifice to defraud, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Jeremiah Reppert, am a Special Agent with the United States Secret Service ("Secret Service"). Based upon my investigation, my review of investigative reports, and my discussions with other individuals involved in this investigation, I have knowledge of the facts below. I describe statements attributed herein to individuals in substance and in part.

1. At all times relevant to this Complaint:

Defendant

a. Defendant DMITRIY SMILIANETS, a/k/a [redacted] a/k/a [redacted] a/k/a [redacted] a/k/a [redacted] a/k/a [redacted] a/k/a [redacted] (hereinafter "SMILIANETS") was a citizen of Russia residing in or near Moscow.

b. SMILIANETS communicated over e-mail using the following accounts, among others: [redacted] ("the Smilic Programmer Account"); [redacted] ("the Smilic [redacted] Account"); [redacted] ("the Smishka [redacted] Account"); and [redacted] ("the Track2 [redacted] Account").

c. SMILIANETS communicated over the ICQ instant messaging service using the account numbers [redacted], [redacted], and [redacted], among others.

Co-Conspirators

d. CC#1 resided in or near St. Petersburg, Russia.

e. CC#2 resided in or near St. Petersburg, Russia.

Victim Banks and Credit Card Companies

f. Hannaford Brothers Co. ("Hannaford") was a regional supermarket chain with stores located in Maine, New Hampshire, Vermont, Massachusetts, and New York that processed credit and debit card transactions through its computer network.

g. Heartland Payment Systems, Inc. ("Heartland"), which was located in or near Princeton, New Jersey and Plano, Texas, among other places, was one of the world's largest credit and debit card payment processing companies. Heartland processed millions of credit and debit transactions daily. Beginning on or about December 26, 2007, Heartland was the victim of a SQL Injection Attack on its corporate computer network that resulted in malware being placed on its payment processing system and the theft of more than approximately 130 million credit and debit card numbers and corresponding Card Data.

h. Citibank, Bank of America and Wells Fargo Bank were "financial institutions" within the meaning of Title 18, United States Code, Section 20.

Computer Intrusion Background

i. Structured Query Language ("SQL") was a computer programming language designed to retrieve and manage data in computer databases.

j. "SQL Injection Attacks" were methods of hacking into and gaining unauthorized access to computers connected to the Internet.

k. "SQL Injection Strings" were a series of instructions to computers used by hackers in furtherance of SQL Injection Attacks.

Shadowcrew

2. Since approximately 2004, the Secret Service has been investigating an international conspiracy to steal money from banks and credit card issuers by obtaining payment card information through various methods, including computer hacking. The conspiracy originally centered around an international organization known as "Shadowcrew," which promoted and facilitated a wide variety of criminal activities including, among others, electronic theft of personal identifying information, payment card fraud, and the production and sale of false identification documents for the purpose of withdrawing stolen funds from bank and credit card accounts.

3. Shadowcrew's website (www.shadowcrew.com) facilitated the commission of the above-referenced crimes by publicly disseminating information regarding how to commit such frauds over electronic forums. The website also permitted the transmission and receipt of private electronic messages between and among Shadowcrew members. Shadowcrew.com also served as an electronic bulletin board for members to advertise and promote the sale of payment card data, stolen bank account information, other stolen personally identifying information, and counterfeit identification documents. Shadowcrew members collectively trafficked in and made unauthorized use of at least 1.5 million stolen payment card numbers, resulting in actual losses in excess of four million dollars to payment card companies, financial institutions, and payment card account holders worldwide.

4. As part of the conspiracy, stolen payment card information was sold to individuals in the United States and in other countries via the Internet. The purchasers of the stolen payment card information would use the account numbers and encode plastic credit cards, which they then would use to withdraw money from automated teller machines ("ATMs") in New Jersey and elsewhere, or to make fraudulent purchases at retail locations, all by purporting to be the authorized accountholders to whom the stolen payment card information had been issued.

Payments for stolen payment card information were often processed via international wire transfer through companies such as Western Union.

[redacted]

5. The Secret Service's investigation has revealed that SMILIANETS registered at www.shadowcrew.com in or about December 2003 using the online nickname (or "nic") [redacted] SMILIANETS provided the Smilic [redacted] Account when he registered at Shadowcrew.com.

6. Between in or about October 2003 and in or about May 2005, SMILIANETS offered stolen payment card information for sale under the nickname [redacted] and trafficked in such information over Shadowcrew.com and over the Internet. The sales and trafficking included, among other instances:

a. In or about October 2003, SMILIANETS used the Smilic [redacted] Account to send approximately 87 payment card account numbers belonging to customers of French and Dutch banks to a Yahoo! e-mail account of a coconspirator in exchange for payment or the promise of payment.

b. On or about December 7, 2003, SMILIANETS advertised that [redacted] had 2 million payment card account numbers in Track 2 format[1] for sale, including numbers from the United States, Europe, and Canada.

c. On or about December 10, 2003, in a private messaging conversation over Shadowcrew.com forum, SMILIANETS and a user nicknamed "Bizman" discussed prices for stolen American and Canadian payment card numbers.

d. On or about December 12, 2003, SMILIANETS stated on a Shadowcrew.com forum that the cards he had advertised for sale on December 10, 2003 to "Bizman" had been stolen from payment card processing centers.

e. On or about July 1, 2004, SMILIANETS used the ICQ account [redacted] to communicate with an individual who, unbeknownst to SMILIANETS, was working at the direction of the Secret Service ("CI"). SMILIANETS offered to send CI a BIN list[1] and

---

[1]Based on my training and experience, I am aware that the magnetic stripe used by credit and debit cards to store data is made up of three separate tracks. Each track stores unique data. Tracks one and two are most commonly used for financial transactions, such as ATM machines and point of sale terminals. Track two includes an account holder's primary account number, expiration date, and service code, among other things.

[1]Based on my training and experience, a "BIN" refers to Bank Identification Number, the first six digits of a credit or debit card number used to identify the issuing bank for a payment card. A BIN

otherwise discussed the sale of payment card data and the fabrication of unauthorized payment cards. Shortly thereafter, CI received an e-mail containing a BIN list from SMILIANETS using the Smilic Programmer Account. The e-mail identified the sender as [redacted]

f. On or about September 5, 2004, SMILIANETS again used ICQ number [redacted] to exchange instant messages with CI. In the conversation, SMILIANETS asked CI whether CI had checked the validity of certain payment card account numbers that SMILIANETS had sent to CI. After CI told SMILIANETS that many of the card numbers provided had been declined, SMILIANETS stated he had just sent approximately 63 more pieces of card data to CI. Shortly thereafter, CI received one e-mail from the Smilic [redacted] Account containing what appear to be the results of SMILIANETS' efforts to check the validity of payment card account numbers. CI also received an e-mail from SMILIANETS containing approximately 78 payment card account numbers over the Track2 [redacted] Account.

g. On or about September 27, 2004 and again several times throughout October 2004, SMILIANETS posted sale and pricing information for payment card data in Track 2 format taken from a card processor.

h. On or about May 24, 2005, SMILIANETS used the Track2 [redacted] Account — the same e-mail account that he used to send payment card data to CI — to send approximately 79 payment card account numbers belonging to customers of banks and credit card issuers in South Korea, Germany, Italy, Sweden, Latvia, France, and the United Kingdom, including customers of BC Card and Samsung Card.

i. On or about May 25, 2005, SMILIANETS' Track2 [redacted] Account received an e-mail from a coconspirator which indicated the password associated with payment for card data that the coconspirator had received was [redacted] which I understand to be a Russian diminutive form for the word or name [redacted]

7. The Secret Service has confirmed with representatives of Citibank, Wells Fargo and Bank of America that several of the payment card account numbers that SMILIANETS sent to CI during the course of the conspiracy belonged to American customers, who suffered fraudulent withdrawals or charges against their accounts.

Defendant Smilianets and V.H.

8. On or about August 7, 2010, V.H. was arrested by French National Police in Nice, France. As part of the arrest, V.H.'s Macbook Pro was seized. Pursuant to a request under a

---

list is offered by providers of stolen payment card data to allow customers to choose cards from certain banks or card issuers.

Mutual Legal Assistance Treaty, French authorities provided a copy of the seized data to the Secret Service. V.H. was also a member of the Shadowcrew organization.

9. Encrypted data V.H.'s Macbook Pro was decrypted by the Secret Service. Results of the subsequent forensic investigation reveal that V.H. was communicating with SMILIANETS via an alias.

a. SMILIANETS was using the alias [redacted] via ICQ chats. The [redacted] alias was tied to ICQ number [redacted]. However, on or about February 26, 2008, SMILIANETS, using the [redacted] alias, in a conversation with V.H., refers to ICQ [redacted] as his other ICQ account. ICQ [redacted] is a known SMILIANETS ICQ number, as discussed above.

b. The [redacted] ICQ number is further tied to SMILIANETS through a chat recovered from computers owned by Albert Gonzalez. Specifically, on or about March 17, 2008, Gonzalez asked a co-conspirator if [redacted] is [redacted]. The co-conspirator replied: "yep." Based on my training and experience, I understand that Gonzalez was asking about "[redacted]" or SMILLIANETS's ICQ number and his co-conspirator confirmed that it was [redacted].

c. Between on or about February 2008 and in or about March 2008, SMILLIANETS, using the [redacted] ICQ number, provided V.H. with an online Webmoney account number of xxxxxxx97822 (the "97822 Account"). SMILLIANETS sent the same 97822 Account number to V.H. from the [redacted] ICQ account, further confirming that SMILLIANETS is [redacted] and [redacted]

10. Between in or about February 2008 and in or about March 2008, using ICQ number [redacted] SMILLIANETS sent V.H. approximately 1,629 credit and debit card number in track 2 format. The card numbers are from various countries including approximately 730 cards from the United States, and cards from Norway, Japan, Italy, Israel, Ireland, Great Britain, Egypt, Canada and others. For example:

a. On or about February 26, 2008, SMILIANETS sent V.H. approximately 143 card numbers, to include cards from Citibank, Chase Bank, and Suntrust Bank in the United States, Lloyds TSB Bank in the United Kingdom, and President's Choice Bank in Canada.

b. On or about March 1, 2008, SMILIANETS sent V.H. approximately 108 card numbers, to include cards from the New Mexico Educators Federal Credit Union and Citibank in the United States.

c. On or about March 26, 2008, SMILIANETS sent V.H. approximately 139 card numbers, to include cards from Citibank in the United States and La Federation des Caisses Desjardins du Quebec in Canada.

11. Between in or about May 2008 and in or about November 2008, SMILIANETS, using ICQ number [redacted] sent V.H. approximately 2,781 card numbers in track 2 format. The card numbers are from various countries including approximately 323 cards from the United States, and cards from Norway, the Italy, Great Britain, France, Sweden, Norway, China, Germany and others. Of these 323 cards from the United States, 5 of them belonged to American Express cardholders living in New Jersey. For example:

a. On or about May 28, 2008 SMILIANETS sent V.H. approximately 74 card numbers to include cards from Discover Bank, Banco Bilbao Vizcaya Argentaria in Spain, Unicredito Italiano in Italy, Sumitomo Mitsui Card Company in Japan, and others.

b. On July 08, 2008 SMILIANETS sent V.H. approximately 117 card numbers, to include cards from Merrill Lynch Bank in the United States, the Bank of Scotland, MBNA Europe Bank Limited, and Barclays Bank in the United Kingdom.

c. On or about November 13, 2008, SMILIANETS sent V.H. approximately 102 card numbers, to include cards from International Card Services in the Netherlands, Commercial International Bank in Egypt, and Europay France.

Central Figure

12. In recorded online chat sessions, SMILIANETS has claimed that in 2004 he had as many as 25,000,000 credit card data breach "dumps" and that in 2005 he had as many as 6,000,000 U.S. credit card data breach "dumps."

13. SMILIANETS has been identified as a central figure in the distribution of data breach dumps, processing greater than 50% of the dumps in the underground market.

The Heartland and Hannaford Intrusions

14. In or about early November 2007, a related company of Hannaford was the victim of a SQL Injection Attack that resulted in the later placement of malware on Hannaford's network and the theft of approximately 4.2 million credit and debit card numbers and corresponding Card Data.

15. Between in or after March 2007 and in or about May 2008, Gonzalez participated in a discussion over an internet messaging service in which one of the participants stated "planning my second phase against Hannaford."

16. Between in or after December 2007 and in or about May 2008, Toey participated in a discussion over an internet messaging service in which one of the participants stated "that's how CC#2 hacked Hannaford."

17. On or about March 17, 2008, Gonzalez asked CC#1 if SMILIANETS resold stolen credit card database dumps given to SMILIANETS by CC#2. CC#1 replied that SMILIANETS was indeed the person processing the credit card dumps.

18. On or about March 17, 2008, Gonzalez asked CC#1, "Do you have any [credit card databases] to sell?" After continued conversation, CC#1 said that he had credit card databases to sell, but that it was really SMILIANETS who was selling the databases for CC#2.

19. On or about December 26, 2007, CC#1 and CC#2 accessed Heartland's computer network by means of a SQL Injection Attack.

20. Between in or about February 2008 and in or about August 2008, SMILIANETS sent "V.H." instant messages providing credit card and debit card numbers obtained by CC#1 and CC#2 from the Heartland and Hannaford hacks.